Mitigating Risks Associated with Digital Ad Fraud

How to beat the bots and fraudsters draining money from your budget.

stirista

Table of Contents

Introduction 3-5

What is digital ad fraud? 6

What are bots? 7-8

What are the types of digital ad fraud? 9-10

How bad is digital ad fraud? 11-12

What's the impact of digital ad fraud on businesses? 13-14

What are the emerging trends in ad fraud? 15-17

Tackling ad fraud 18-21

How we address ad fraud 22

Picture This

You've launched a programmatic digital ad campaign to outstanding, almost unbelievable success. With so many impressions and clicks, it almost seems too good to be true.

Maybe This.

You take a closer look at the analytics. While clicks are sky-high, you notice surprisingly few users actually converted during the campaign. Weird

Could it be that all those clicks, rather than coming from human users interacting with your content, actually came from bots? Could it be that those metrics are inflated, and therefore wrong–instead, revealing that your ad dollars were stolen, right under your nose? Could you be a victim of ad fraud?

What's more terrifying is that ad fraud is rarely that readily apparent–and in the long run, *all advertisers* are victims of ad fraud. In fact, a report from Juniper Research states that

22% | **of all ad spending in 2023 could be attributed to fraud.[1]**

[1]https://www.prnewswire.com/news-releases/new-ad-fraud-study-22-of-online-ad-spend-is-wasted-due-to-ad-fraud-in-2023-according-to-juniper-research-301938050.html

Ad Fraud is Insidious

It's typically undetectable, especially without readily designed tools made especially for the job. As a result, fraudsters are able to divert a significant amount of money away from ad budgets.

According to Statista, digital ad fraud worldwide cost businesses $84 billion in 2023. By 2028, that number is expected to be over $172 billion. That's roughly a 14% increase each year.[2]

Scammers sunk their claws into the industry long ago-and they continue to expand their reach into advertising, especially as programmatic buying grows. Programmatic advertising currently makes up over 90% of US digital display advertising, up from 86% in 2019.[3]

Because advertising represents a significant investment for marketers-and because of the complex nature of programmatic-ad fraud is one of the biggest hurdles facing marketers, publishers, and advertisers today. And with fraudsters attacking new industries and using new tools powered by generative AI, attempts to steal advertising budgets are becoming increasingly sophisticated-and widespread.

According to Statista

$84 Billion

cost businesses of digital ad fraud worldwide in 2023

Over

90%

makes up programmatic advertising currently.

[2]https://www.statista.com/statistics/677466/digital-ad-fraud-cost
[3]https://www.emarketer.com/content/programmatic-ad-spending-set-reach-nearly-180-billion-by-2025

So How do you Stop Massive Amounts of Money From Being Drained from Your Ad Budget Each Year?

In this report, we'll teach you all about ad fraud-including what it is, what it looks like, and how to best protect against it.

What is digital ad fraud?

In a nutshell, digital ad fraud is the process of distorting digital advertising metrics–like click-through rates and impressions–to deceitfully generate revenue by siphoning money away from advertisers.

Ad fraud makes it seem like ads are being seen or engaged with by real users, but in reality, those impressions are typically generated by bots or even employees paid to repeatedly click on ads.

Fake clicks, fake views, and even fake conversions are all capable of undermining the best efforts of your marketing team.

What are bots?

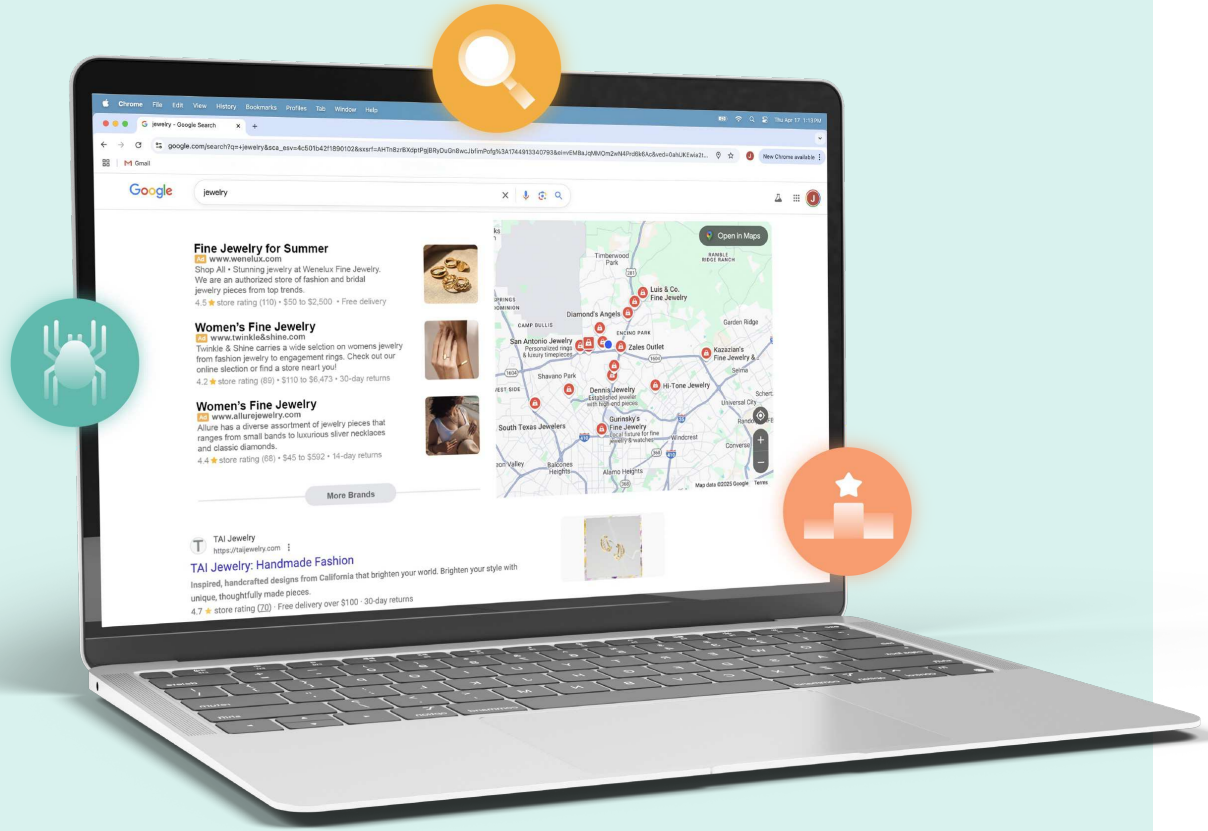
Fraudsters exploit the automated processes of programmatic advertising in order to drain ad budgets and skew campaign metrics, all while diminishing campaign effectiveness. Their most common weapon of choice, perfect for a programmatic environment? Bots.

Bots are software programs designed to mimic human behavior. They are capable of doing everything from simulating clicks and impressions to mimicking complex user interactions on websites, especially with the advent of generative AI. Because they operate across multiple networks and devices, bots are difficult to detect–yet the metrics they manipulate noticeably draw budgets away from genuine user engagement.

Good Bots vs. Bad Bots

Good Bots

Good bots are programs like search engine crawlers, which visit websites to find content in order to populate search engine query results. Other types of good bots monitor site performance.



Bad Bots

The 2024 Bad Bot Report from Imperva attributes **half of all internet traffic to bots**.

32% | **of which are bad bots.**[4]

Bad bots, on the other hand, are those that generate fake clicks and impressions–mimicking human behavior in order to seem like they're producing real interactions. These are the bots digital advertisers want to snuff out. But as bot-detecting technology improves, so do fraudsters' bots.

It's Important to Note:

Good bots can also skew analytics reports by generating their own impressions. Therefore, it's important to distinguish human impressions not only from the bad bots, but from the good bots, too.

[4]https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/

What are the Types of Digital Ad Fraud?

There are many types of ad fraud–in fact, the types and variants of ad fraud continue to grow year after year. That said, here are the most common types of ad fraud, which you'll typically encounter in a digital campaign:

Ad Stacking

Similar to impression fraud in that ads are hidden, ad stacking involves stacking multiple ads on top of one another in a single ad placement, with only the topmost ad visible to users. However, each click or impression is counted for every ad in the stack. As a result, advertisers pay for impressions or clicks on hidden ads–resulting in wasted ad spend.

Impression Fraud

Impression fraud involves, again, the use of bots to generate fake impressions on digital ads. This time, the bots load ads in unseen spaces or on hidden pages, yet make it seem as if real users are viewing the ads. These bots inflate the total number of ad views in reports, skewing campaign metrics.

Domain Spoofing

Domain spoofing occurs when fraudsters pretend that low-quality or fake websites are premium publishers to trick advertisers. They manipulate ad exchanges to misrepresent the quality and authenticity of the ad placement, sometimes using URLs that resemble known websites, and as a result, advertisers are tricked into paying high rates for ad inventory on sites that only appear to be reputable–yet in reality, are quite the opposite.

Click Fraud

One of the most common types of ad fraud, click fraud involves the use of bots, or even human teams, that generate fake ad clicks on online ads. They are typically used in pay-per-click campaigns, thereby inflating ad costs by charging for each fake click.

Bot Traffic

Bot traffic refers to any non-human traffic on a website or app. Different bots perform different tasks. As we discussed, bad bots perform automated tasks that mimic human behavior, skewing analytics by reporting nonhuman impressions.

Pixel Stuffing

With pixel stuffing, digital ads are placed on tiny areas on a website, typically within a 1x1 pixel area. The ad is pretty much invisible to the human eye but is still reported as a delivered ad–making all the impressions on these ads fraudulent.

How Bad is Digital Ad Fraud?

The world of digital ad fraud is an attractive one to fraudsters. With the growth of programmatic, the advent of new tools like generative AI, and the ability to attack new channels and devices, the risk of fraud has risen across the board. And fraud detection processes struggle to keep up.

One out of five marketers

in the US considers ad fraud a challenge.[5]

And in 2021, **almost 18%** of ad impressions served programmatically in the US were fraudulent.[6]

Back in 2016, the World Federation of Advertisers predicted that, in the course of ten years, ad fraud and similar schemes would become the second-biggest market for organized crime. An estimate from the study put the level of ad fraud at $50 billion for 2025, which would've been equal to 10% of the total ad market.[7]

Now, we know those numbers were far too conservative in their estimates–though the percentage of ad fraud to total market share is roughly the same. The cost of ad fraud in 2025 is estimated to be over $100 billion, while the worldwide ad market is estimated to exceed $1 trillion.[8,9]

[5]https://www.statista.com/statistics/1092685/display-advertising-challenges/
[6]https://www.statista.com/statistics/677466/digital-ad-fraud-cost/#:~:text=Fraud%20in%20advertising%20%E2%80%93%20costs%20and%20concerns&text=In%202021%2C%20close%20to%2018,consider%20ad%20fraud%20a%20challange.
[7]https://wfanet.org/knowledge/item/2016/06/06/WFA-issues-first-advice-for-combatting-ad-fraud
[8]https://www.emarketer.com/content/worldwide-ad-spending-forecast-2025
[9]https://www.statista.com/statistics/677466/digital-ad-fraud-cost/#:~:text=It%20was%20estimated%20that%20the,a%20growing%20risk%20of%20fraud.

Projected Losses

While **ad fraud may cost businesses over $172 billion in 2028**, that number may be even higher if nothing is done about it–especially with AI giving fraudsters new tools and avenues for fraud.

According to a report from DoubleVerify, the advent of generative AI will embolden fraudsters to increase the types and numbers of ad fraud schemes. The research from DoubleVerify revealed a 23% increase in new fraud schemes compared to the previous year. It also revealed that fraudsters are shifting their schemes to include CTV and streaming audio.[10]

With generative AI, it's becoming easier for fraudsters to falsify data patterns, better mimicking human behavior. However, good AI can fight bad AI–and advancements in machine learning mean that ad fraud detection tools may be able to catch up to fraudsters' advanced tactics, too.

[10]https://ir.doubleverify.com/news-events/press-releases/detail/297/doubleverify-gen-ai-driving-significant-increase-in-new-ad

What’s the Impact of Digital Ad Fraud on Businesses?

Beyond the obvious monetary cost of digital fraud on businesses, there’s also the loss of good data analytics, which leads to less actionable insights, and damage to brand reputation.

Financial Loss

This one is clear enough. Fraudsters' main goal is to steal money directly from advertisers' budgets. Yet the money being stolen in ad fraud not only represents the initial loss in the ad budget, but a loss in the future ability to make informed marketing decisions. As a result, the financial loss a company experiences becomes a compounding loss the longer ad fraud remains unaddressed.

Wasted Ad Spend

Ad money that could've fueled genuine user interactions gets spent on interactions that reach no one, instead padding the pockets of fraudsters. Not only that, but that wasted ad spend can increase the longer ad fraud remains undetected–after all, seemingly "good" numbers of impressions and clicks can encourage advertisers to put more of their ad budget into those channels, the longer they fail to realize that all those impressions likely came from bots.

Skewed Data

The reality is that your dollars may be going to ad fraud. But how can you know which dollars are being siphoned by fraudsters? Because digital ad fraud leads to misleading analytics, KPIs become skewed. As a result, marketers can't measure the effectiveness of their campaigns–or will make inaccurate assessments based on the inaccurate data. Inaccurate insights lead directly to misinformed decisions, and thus budgets may get redirected toward ineffective strategies.

Damage to Brand Reputation

Fraud can link brands to poor-quality websites filled with malicious content, damaging that brand's reputation and credibility. Negative perceptions of the brand can arise among consumers and stakeholders alike.

What are the Emerging Trends in Ad Fraud?

Ad fraud is constantly evolving as fraudsters adapt to new detection methods and incorporate emerging tools. According to DoubleVerify, there was a 23% surge in new ad fraud schemes and variants in 2023 compared to 2022.

Here are some of the top ways fraudsters are improving their fraud schemes.

Sophistication of Techniques

AI in Ad Fraud

Fraudsters are now using AI and machine learning to mimic human behavior and better falsify data patterns–as a result, bot activity is harder to detect. Fraudulent engagement now looks a lot more realistic.

First-Party Data Manipulation

As third-party cookies go away, fraudsters are exploiting first-party data, trying to create synthetic IDs and fake user profiles to manipulate ID-based ad targeting–a tactic that's much easier now with generative AI.

Blockchain-Based Ad Fraud

While blockchain can also serve as a fraud prevention tool, fraudsters are also finding ways to exploit it. Fake blockchain-based verification systems are emerging, deceiving advertisers who think they're using a secure method.

Targeting New Channels and Platforms

CTV & OTT

Fraud tactics in CTV include device spoofing, server-side ad insertion (SSAI) fraud, and fake CTV apps that generate fraudulent impressions.

Consider the 2021 case of the ParrotTerra scam, a server-side ad inversion online fraud scheme. At its peak, the scheme spoofed over 20 million CTVs in order to deceive advertisers into believing they were provided with a large CTV ad inventory.[11]

[11]https://www.adexchanger.com/digital-tv/doubleverify-uncovers-largest-ctv-ad-fraud-scheme-to-date/

Retail Media Networks

With brands pouring money into Walmart Connect, Amazon Ads, Instacart Ads, and Target Roundel, these retail media networks are becoming lucrative ad fraud targets. Fraudsters can create bots that mimic shopping behavior to trigger attribution, and fake clicks can also be inserted right before a real purchase to steal credit.

Social Media & Influencer Marketing

Fake influencer engagement is also emerging, and we're talking more than deepfakes. Bots can inflate likes, comments, and video views–and also sell fake followers to accounts. Because platforms like TikTok, Instagram, and YouTube are gaining in popularity, advertisers are driven to spend on these channels–yet these platforms offer weak fraud detection.

Tackling Ad Fraud?

In many cases, outsmarting fraudsters involves staying on top of their schemes and trying to one-up their latest techniques with new developments. If they're using generative AI and machine learning, that means using those same tools to detect their AI-generated traffic.

Use AI and Machine Learning

Just because ad fraud techniques are getting more sophisticated doesn't mean techniques to combat ad fraud are falling behind. In fact, tools like AI and machine learning can help combat ad fraud.

By processing vast amounts of data at high speeds, algorithms can detect patterns that a human might overlook. Anomalies in click rates, suspiciously timed impressions, and more can all be detected through machine leaning tools.

Pattern Recognition

AI models can be trained to recognize patterns in data that correspond to fraudulent behaviors. These models will learn from the new data, continually improving detection capabilities. These systems can also detect anomalies in data patterns–perhaps identifying fraud by looking at specific IP ranges or activity coming from dormant accounts.

Predictive Analytics

Machine learning tools can forecast potential fraud activities based on historical trends.

Use Ad Verification Tools

Ad verification tools can help make sure your ads are appearing on trusted websites, and can also help detect invalid traffic, bots and suspicious activity.

Monitor Traffic Quality

Real-time monitoring allows you to continuously monitor your advertising campaign to detect and respond to threats. That way, you minimize the time fraudsters have to cause damage.

You can also use filters to screen out low-quality traffic sources and block known bot traffic–and exclude them from traffic reports.

Work With Trusted Partners

Limit your exposure to spaces where fraudsters can run rampant by only working with trusted vendors, publishers, and ad networks–and with those who invest in technology and practices that detect and prevent ad fraud.

Professional marketing agencies can also recommend platforms and networks that employ anti-fraud measures and value transparency.

How We Address Ad Fraud

Stirista deals with ad fraud through a number of partnerships and processes, ensuring our partners can always place ads and launch campaigns confidently.

In 2024, we launched a multi-year partnership with Pixalate, a leading platform in ad fraud protection for CTV, mobile advertising, and websites. Through our Pixalate partnership, we've been able to take a proactive approach to ad transparency, achieving high records of fraud prevention for programmatic media buying–CTV and display included.

Through Pixalate, we offer our clients reliable Invalid Traffic (IVT) detection and a bot filtration system to ensure impressions are always legitimate. Altogether, we protect your ad dollars and ensure your campaign analyses are always accurate and actionable.

How Stirista Address Ad Fraud

At Stirista, we understand that the landscape of digital advertising is rife with hidden challenges, and ad fraud stands as a significant threat to the effectiveness of any marketing campaign. That's why we've positioned ourselves as more than just a media buying partner; we're your dedicated anti-fraud ally. We recognize that true marketing success hinges on the integrity of your data and the authenticity of your audience engagement. To this end, we've built our approach on a foundation of unwavering transparency and trust.

We Go Beyond Surface-Level Metrics

Diving deep into the intricate mechanisms of programmatic advertising to ensure that every impression, click, and conversion is genuine. Our commitment is to deliver fraud-free marketing solutions across all programmatic spaces, providing you with the peace of mind that your investments are reaching real people, not bots or fraudulent entities. We meticulously scrutinize every stage of a campaign, employing advanced technologies and rigorous verification processes to identify and eliminate fraudulent activity. This proactive approach allows us to safeguard your budget and maximize your ROI, ensuring that your marketing efforts translate into tangible business results.

With Stirista, you can be confident that you're partnering with a team that prioritizes the authenticity and effectiveness of your advertising initiatives.

Learn How Stirista Can Help!

Contact us today:
210-293-0029
info@stirista.com

stirista

1641 San Pedro Ave., Suite 150 San Antonio, TX 78232